Chapter 55: Technology and Strategic Services

Rule 55.1 Technology and Strategic Services
1. The Office of Technology and Strategic Services (OTSS) is to ensure appropriate authorized access of IT resources and services, equipment and usage for the security and protection of information as assigned by State of Mississippi. These resources are provided to conduct and support state business and educational functions as required by law. OTSS provides security and controls to enhance efforts in providing confidentiality, integrity and availability to the departments within MDE as with student and personnel information in schools, public and nonpublic school districts governed by the State Board of Education. All information technology assets that are managed, operated, maintained, or in the custody or proprietorship of the agency and/or hosted by third parties on behalf of MDE must be utilized to ensure:

   a. Appropriate Use
   b. Availability
   c. Accountability
   d. Data Integrity
   e. Privacy and Confidentiality

   Employees and authorized users are required to adhere to the "Appropriate and Acceptable Use Policy" that is published in the MDE Human Resource Employee Policy and Procedures Manual and on the OTSS website. Users must read and acknowledge the policy as a condition of being granted access to Office of Technology and Strategic Services' technology assets during their tenure as an employee or authorized user. Users will be held responsible for protection of all technology resources and information for which they are entrusted and using them for their intended purposes.
   The Office of Technology and Strategic Services Security Policy has been created as a directive of MS Information Technology Services as it applies in MS Code 25-53-1 to §25-53-25. Each agency must establish a framework to operate, develop, implement and apply appropriate security measures to protect and safeguard the agency and its users from forms of unauthorized access, malicious misuse, disclosure, modification or inadvertent compromise.

   State board governed schools, public and non-public school districts are required to create a district wide Information Technology Security Policy. The policy will develop, implement and maintain district information technology resources that are managed, operated or in the custody or proprietorship of the district and/or MDE and/or hosted by third parties on behalf of the school district and/or MDE. The requirements and standards cannot be less than those established in the OTSS Information Technology Security Policy.

   The more restrictive policy will take precedence in the event of a conflict between the agency's policy and the district's policy.

2. Information Technology Steering Committee (ITSC)
The Information Technology Steering Committee is established to be the coordinating body for the agency and school districts technology resources and information security- related activities. It is composed of appointed staff from the Office of Technology and Strategic Services and

representatives appointed by the State Superintendent of Education and/or a Deputy Superintendent of Education.

3. ITSC responsibilities include:
Assisting the Chief Information Officer (CIO) in developing, reviewing, and recommending technology resources and information security policies for the agency and all governed school districts by the board
Identifying and recommending industry best practices for technology asset usage and information security
Developing, reviewing, implementing and recommending federal and statewide standards, procedures and guidelines
Coordinating inter-departmental and school district professional and accurate communication and collaboration on technology usage, security issues and future access system changes
Coordinating statewide information technology and security education and awareness to all governed school districts by the state board

Source: *Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards Technology (NIST), Federal Information Processing Standards 200 (FIPS)*
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g; 34 CFR Part 99)
No Child Left Behind Act of 2001, The Individuals with Disabilities Education Improvement Act of 2004 (IDEA)34CFR 300.560-300.577, The U.S. Department of Agriculture – Use of Free and Reduced Price Meal, Eligibility Information Nondiscrimination or Identification of Recipients, 42USC 1758 (b)(2)(C)(iii), Richard B Russell National School Lunch Act (42U.S.C. 1751 et seq.)
The Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.),
Miss. Code Ann. §37-1-3, 37-3-5, §37-151-9, §25-53-1 to §25-53-25 (Revised 4/2016)

Chapter 55: ~~Office of~~ Technology and Strategic Services

Rule 55.1 ~~Office of~~ Technology and Strategic Services
4. The Office of Technology and Strategic Services (OTSS) is to ensure appropriate authorized access of IT resources and services, equipment and usage for the security and protection of information as assigned by State of Mississippi. These resources are provided to conduct and support state business and educational functions as required by law. OTSS provides security and controls to enhance efforts in providing confidentiality, integrity and availability to the departments within MDE as with student and personnel information in schools, public and nonpublic school districts governed by the State Board of Education. All information technology assets that are managed, operated, maintained, or in the custody or proprietorship of the agency and/or hosted by third parties on behalf of MDE must be utilized to ensure:

    f. Appropriate Use
    g. Availability
    h. Accountability
    i. Data Integrity
    j. Privacy and Confidentiality

    Employees and authorized users are required to adhere to the "Appropriate and Acceptable Use Policy" that is published in the MDE Human Resource Employee Policy and Procedures Manual and on the OTSS website. Users must read and acknowledge the policy as a condition of being granted access to Office of Technology and Strategic Services' technology assets during their tenure as an employee or authorized user. Users will be held responsible for protection of all technology resources and information for which they are entrusted and using them for their intended purposes.
    The Office of Technology and Strategic Services Security Policy has been created as a directive of MS Information Technology Services as it applies in MS Code 25-53-1 to §25-53-25. Each agency must establish a framework to operate, develop, implement and apply appropriate security measures to protect and safeguard the agency and its users from forms of unauthorized access, malicious misuse, disclosure, modification or inadvertent compromise.

    State board governed schools, public and non-public school districts are required to create a district wide Information Technology Security Policy. The policy will develop, implement and maintain district information technology resources that are managed, operated or in the custody or proprietorship of the district and/or MDE and/or hosted by third parties on behalf of the school district and/or MDE. The requirements and standards cannot be less than those established in the OTSS Information Technology Security Policy.

    The more restrictive policy will take precedence in the event of a conflict between the agency's policy and the district's policy.

5. Information Technology Steering Committee (ITSC)
The Information Technology Steering Committee is established to be the coordinating body for the agency and school districts technology resources and information security- related activities. It is composed of appointed staff from the Office of Technology and Strategic Services and

representatives appointed by the State Superintendent of Education and/or a Deputy Superintendent of Education.

6. ITSC responsibilities include:
Assisting the Chief Information Officer (CIO) in developing, reviewing, and recommending technology resources and information security policies for the agency and all governed school districts by the board
Identifying and recommending industry best practices for technology asset usage and information security
Developing, reviewing, implementing and recommending federal and statewide standards, procedures and guidelines
Coordinating inter-departmental and school district professional and accurate communication and collaboration on technology usage, security issues and future access system changes
Coordinating statewide information technology and security education and awareness to all governed school districts by the state board

Source: *Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards Technology (NIST), Federal Information Processing Standards 200 (FIPS)*
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g; 34 CFR Part 99)
No Child Left Behind Act of 2001, The Individuals with Disabilities Education Improvement Act of 2004 (IDEA)34CFR 300.560-300.577, The U.S. Department of Agriculture – Use of Free and Reduced Price Meal, Eligibility Information Nondiscrimination or Identification of Recipients, 42USC 1758 (b)(2)(C)(iii), Richard B Russell National School Lunch Act (42U.S.C. 1751 et seq.)
The Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.),
Miss. Code Ann. §37-1-3, 37-3-5, §37-151-9, §25-53-1 to §25-53-25 (Revised 4/2016)